UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,409	12/04/2003	Richard C. Johnson	ORCL5881	7705

53156 7590 03/24/2006

YOUNG LAW FIRM, P.C.
4370 ALPINE RD.
STE. 106
PORTOLA VALLEY, CA 94028

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 03/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/727,409	JOHNSON, RICHARD C.	
	Examiner	Art Unit	
	Charlie C. Agwumezie	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2003*.

2a)☒ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5, 7-13, 15-24, and 27-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-13,15-24 and 27-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/17/03; 8/15/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. Claims 6, 14, 25, and 26, are cancelled. Claims 1, 9, and 20, are amended. Claims 29, 30-33 are newly added. Claims 1-5, 7-13, 15-24, and 27-33, are pending in this application per the response to office action filed January 11, 2006.

Response to Arguments

2. Applicant's arguments with respect to claim 1-5, 7-13, 15-24, and 27-33, have been considered but are moot in view of the new ground(s) of rejection.

3. However Applicant's argument that Brown's repository of digital certificate does not meet the requirements of amended claim 1 so that the authority of the user is independent of the digital certificate is in error. Applicant however conceded that Brown only discloses checking the digital certificate for the certificate holder's maximum signing authority, Applicant still concluded that does no teach that the authority of the user is verifiable by accessing a store of authority that is independent of the digital certificate as claimed. Applicant further argued that no independent validation of any authority information is carried out or taught in Brown et al.

In response the Examiner respectfully disagrees with the Applicant characterization of Browns digital certificate. Brown's digital certificate is preferably issued by a trusted third party referred to as certificate authority (0164) with tags (figs.1 and 3) namely (to be signed tag, accessible by tag and/or role identifier). The role identifier includes an authenticator (validator) which is used to authenticate signer's

identity, as well as the signer's authorization (signer's rights) to sign the document in the specified role (0067). This authentication and/or validation is independent of the received digital certificate from the certificate authority which came with the various tags to be fetched. Thus Brown's certificate does meet the requirements of amended claim 1 so that the authority of the user is independent of the digital certificate as claimed. Furthermore of what use is a digital certificate that does not require validation and/or authentication as Applicant appear to portray.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 9-13, and 15-19**, are rejected under 35 U.S.C. 102(e) as being anticipated by Brown et al U.S. Patent Application Publication No. 2004/0139327 A1.

5. As per **claim 9**, Brown et al discloses a computer-implemented method for ensuring non-repudiation of a payment request, the payment request being generated in a computing environment having a connection to a network, the method comprising the steps of:

receiving, over the network, the payment request together with a certificate identifying a user having caused the payment request to be generated, the certificate including certificate-identifying information and user-identifying information, the certificate further including authority information defining an authority of the user to make the payment request (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80);

validating the certificate-identifying information and the user-identifying information included within the received certificate by accessing a store of authority information that is independent of the received certificate (figs. 1, 2, 3, and 8; 0165; 0067; 0174; 0183; claim 80);

validating the authority information included within the received certificate, and executing of the payment request only when the certificate-identifying information, the user-identifying information and the authority information within the received certificate is successfully validated (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80).

6. As per **claim 10**, Brown et al further discloses the method, wherein the payment request is for a predetermined amount and wherein the payment request is authorized only when the validating steps are successful and when the authority information for the user stored in the hierarchical authority data structure lists an authorized amount for the user at least equal to the predetermined amount (0177; 0183; 0184; 0185).

7. As per **claim 11 and 16**, Brown et al further discloses the method, wherein the certificate received in the receiving step conforms to the X.509 standard (0109; 0164;

0183).

8. As per **claim 12 and 17**, Brown et al further discloses the method, wherein the authority information is configured as XML code (0062; 0068; 0069).

9. As per **claim 13 and 18**, Brown et al further discloses the method, wherein the XML code is compliant with a DSML standard (0062; 0068; 0069).

10. As per **claim 15**, Brown et al discloses a software application configured to carry out a financial transaction, the application being configured to run on a computer coupled to a network, and comprising, stored on a computer-readable medium:

certificate receiving code which is configured to receive a digital certificate from a user over the network, the certificate including certificate-identifying information and user-identifying information, the certificate further including authority information that defines an authority granted to the user to request that the financial transaction be carried out (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80);

certificate validating code configured to enable validation of the certificate-identifying information and user-identifying information within the received certificate, and authorization validating code configured to enable validation of the authority information within the received certificate against corresponding authority information for the user stored in a data structure that is independent of the received certificate (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80).

11. As per **claim 19**, Brown et al further discloses the software application, wherein the authority defined by the authority information within the received certificate also defines rights of the user to access predetermined data and programs within the network (0183; 0184).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 1-8 and 29-33**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown et al U.S. Patent Application Publication No. 2004/0139327 A1 in view of Hwangbo U.S. Patent Application Publication No. 2003/0154376 A1.

13. As per **claim 1 and 29**, Brown et al discloses in a computing environment having a connection to a network, computer readable code readable by a computer system in said environment, for enabling a server computer within the computing environment to both authenticate a user of a client computer within the computing environment and to verify that the user is authorized to request that the server computer carry out a requested action, comprising:

a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field;

wherein the second code portion of the digital certificate is configured to define an authority of the user of the client computer to request that the server computer carry out the requested action, the second code portion being configured for inclusion within the extension field of the first code portion, the authority of the user defined within the second code portion of the certificate being verifiable by the server computer independently of the digital certificate by accessing a store of authority information that is independent of digital certificate (see figs. 1 and 3; 0165; 0067; 0174; 0183).

What brown does not explicitly teach is a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field.

Hwangbo discloses a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial

number, a certificate validity period, a digital signature of the certificate authority, and the extension field (fig. 10; 0029; 0034; 0096; claim 17).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Brown et al and incorporate a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field as taught by Hwangbo, in order to show details and or configurable nature of X.509 and its capabilities.

14. As per **claim 2 and 30,** Brown et al further discloses a computer readable code, wherein the digital certificate conforms to the X.509 standard (0109; 0164; 0183).

15. As per **claim 3 and 31**, Brown et al further discloses the computer readable code, wherein the second code portion is configured as XML code (0062; 0068; 0069).

16. As per **claim 4 and 32**, Brown et al further discloses the computer readable code, wherein the XML code is compliant with a DSML standard (0109; 0164; 0183).

17. As per **claim 5 and 33**, Brown et al further discloses the computer readable code, wherein the authority of the user of the client computer is stored in a hierarchical

authority data structure that is accessible by the server computer (0183).

18. As per **claim 6**, Brown et al further discloses the computer readable code, wherein the authority of the user defined within the second code portion of the certificate is verifiable by the server computer accessing a store of authority information that is independent of the received certificate (0183).

19. As per **claim 7**, Brown et al further discloses the computer readable code, wherein the authority defined within the second code portion defines access rights of the user to data and programs within the computing environment (0183).

20. As per **claim 8**, Brown et al further discloses the computer readable code, wherein the authority defined within the second code portion defines rights of the user to issue payment requests (0183; see claim 80).

21. **Claims 21-23,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter et al, U.S. Patent Application Publication No. 2005/0060584 in view of Brown et al U.S. Patent Application Publication No. 2004/0139327 A1

22. As per **claim 21**, Ginter et al failed to explicitly disclose the computer-implemented method, wherein the primary and secondary certificates conform to the X.509 standard.

Brown et al discloses the computer-implemented method, wherein the primary and secondary certificates conform to the X.509 standard (0109; 0164; 0183).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Ginter et al and incorporate a method, wherein the primary and secondary certificates conform to the X.509 standard as taught by Brown et al in order to show details of implementation and certificate format used.

23. As per **claim 22**, Ginter et al failed to disclose the computer-implemented method, wherein the primary and secondary authority information are encoded within the primary and secondary certificates as XML code

Brown et al discloses the computer-implemented method, wherein the primary and secondary authority information are encoded within the primary and secondary certificates as XML code (0062; 0068; 0069).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Ginter et al and incorporate a method, wherein the primary and secondary authority information are encoded within the primary and secondary certificates as XML code as taught by Brown et al in order to show details of implementation and data format used.

24. As per **claim 23**, Ginter et al failed to explicitly disclose the computer-implemented method, wherein the XML code is compliant with a DSML standard.

Brown et al discloses the computer-implemented method, wherein the XML code is compliant with a DSML standard (0109; 0164; 0183; 0085).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Ginter et al and incorporate a method, wherein the XML code is compliant with a DSML standard as taught by Brown et al in order to show format used.

25. **Claims 20, 24, and 27-28**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter et al U.S. Patent Application Publication No. 2005/0060584 in view of Samar U.S. Patent Application Publication No. 2002/0078355 A1.

26. As per **claim 20**, Ginter et al discloses a computer-implemented method for controlling authority of employees of a company within in a computing environment, the company having a hierarchical management structure, the method comprising the steps of:

creating or receiving a primary digital certificate, the primary digital certificate including primary authority information that defines and grants primary rights to a primary employee as defined by the hierarchical management structure (see fig. 50; 0320; 0907; 0572; 0917; 1136);

creating secondary digital certificates and assigning the created secondary certificates to selected secondary employees requiring access to the computing environment, each of the selected secondary employees occupying a predefined

position within the hierarchical management structure that is hierarchically lower than that of the primary employee, each of the secondary certificates including secondary authority information that defines and grants secondary rights, the secondary rights being derivative from the primary rights and being commensurate with the predefined position of the selected secondary employee within the hierarchical management structure (0917; 0907; 0908; 1136 "it may be efficient and/or desirable for each institution holding certificate to issue dependent certificate to its own faculty, staff and students" and "certifying authority may issue electronic controls, subject to the controls issued by rights holder for example, that delegate, to the institution's certifying authority the authority and responsibility to issue dependent certificates within certain limits"), and

allowing each selected secondary employee to exercise only those rights within the computing environment that are granted by the secondary rights defined within the assigned secondary certificate (0293; 0406; 0910; 0888; 1203; see claim 67).

What Ginter et al does not explicitly teach is

revoking a secondary certificate to a terminated secondary employee, the revoking step being operative to revoke all certificates to secondary employees of the company that report to the terminated secondary employee, and to revoke all secondary rights that are derivative from the secondary rights granted by the revoked secondary certificate. Ginter et al however discloses that "it may be efficient and/or desirable for each institution holding certificate to issue dependent certificate to its own faculty, staff and students" and "certifying authority may issue electronic controls, subject to the controls issued by rights holder for example, that delegate, to the institution's certifying

authority the authority and responsibility to issue dependent certificates within certain limits. Thus it would have been obvious that revocation of dependent certificate revokes all derivatives rights of the secondary holder.

Samar discloses revoking a secondary certificate to a terminated secondary employee, the revoking step being operative to revoke all certificates to secondary employees of the company that report to the terminated secondary employee, and to revoke all secondary rights that are derivative from the secondary rights granted by the revoked secondary certificate (0009; 0011).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Ginter et al and incorporate a method, revoking a secondary certificate to a terminated secondary employee, the revoking step being operative to revoke all certificates to secondary employees of the company that report to the terminated secondary employee, and to revoke all secondary rights that are derivative from the secondary rights granted by the revoked secondary certificate as taught by Samar in order ensure proper use of the certificate by saving cost misuse.

27. As per **claim 24**, Ginter et al further discloses the computer-implemented method, wherein the secondary rights defined within at least one of the secondary certificates are derivative from secondary rights defined within another secondary certificate (0907; 0908; see claim 67 and 68).

28. As per **claim 27**, Ginter et al further discloses the computer-implemented

method, wherein the primary and secondary rights define access rights to data and programs within the computing environment (0293; 0606).

29. As per **claim 28**, Ginter et al further discloses the computer-implemented method, wherein the primary and secondary rights each define amounts to which the primary and each of the secondary employees, respectively, are authorized to bind the company (see claim 52 and 60).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art ad are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of

the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charlie C. L. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on **(571) 272 – 6712**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington D.C. 20231

Or faxed to:

(571) 273-8300. [Official communications; including After Final communications labeled "Box AF"].

(571) 273-8300. [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"].

Hand delivered responses should be brought to the United States Patent and Trademark Office Customer Service Window:

Randolph Building,

401 Dulany Street

Alexandria VA. 22314

Charlie Lion Agwumezie
Patent Examiner
Art Unit 3621
March 14, 2006

PRIMARY EXAMINER